In March of 2009, my office was contacted by Attorney [redacted] in Fresno California in regards to the case of United States vs. [redacted]. Attorney [redacted] requested the assistance of my office in performing a forensic examination on media seized by the government from Mr. [redacted] as a result of a search warrant executed at his residence in December of 2007. This search warrant had been obtained through the preparation of an affidavit of probable cause by Immigration and Customs Enforcement SSA Craig Finley. I have been provided a copy of this affidavit by Attorney [redacted]'s office for review. In particular I was asked to review the affidavit as to its specificity in associating the offense of purchasing child pornography to the defendant Mr. [redacted]. The affidavit goes into great detail regarding the Immigration and Customs investigative efforts into certain web sites distributing child pornography. It also goes into some detail as to how Internet Protocol (IP) addresses are used to link specific computers (and their physical location) to illegal activity on the Internet, it does not actually do so as it pertains to Mr. [redacted].

ANALYSIS OF PROBABLE CAUSE

An Internet Protocol (IP) address is similar to a residential address for a home or business. Every computer connected to the Internet must have its own unique IP address for the Internet to work correctly. Just as a residential address must include a zip code, state, city, street and house number for a piece of mail to arrive at its door, a computer connected to the Internet must also have an individual set of numbers, unique unto itself to receive (or send) information across the Internet.

IP addresses can be "static" or "dynamic". Static IP addresses remain the same for periods of time and are commonly associated with such things as a business's cable connection to the Internet that might include not only access to the Internet but the company web page as well. Dynamic IP addresses are "dynamic" in that they change, sometimes, every time the computer user re-accesses the Internet. Dial-up accounts such as those through America On-Line are an example of this but many cable connections (ala Comcast) are in a sense "dynamic" in that they are leased lines and may or may not change from household to household over time.

For law enforcement purposes involving tracking illegal activity on the Internet IP addressing is critically important and the key to determining from what physical location a particular illegal activity is occurring. I noted on page 9 of SSA Finley's search warrant affidavit that he accurately describes what an IP address is and notes that "each time an individual accesses the Internet, the computer from which that individual initiates access is assigned an IP address" (Page 9 lines 6 through 9).

This statement is correct because not knowing the IP number associated with the illegal activity makes it unlikely that the investigator will be able to determine a particular physical location (and hence a suspect) from where the activity originated.

When the investigator does know the IP address in question they must first determine what entity "owns" (or typically leases) that address (IE Comcast, Quest, AOL etc.) and after contacting that entity, determine if the IP address is static or dynamic.

If the IP address associated with the illegal activity is static, the investigator can determine via subpoena or summons who the subscriber of the IP address is and the physical address of that connection. If the IP address associated with the illegal activity is dynamic, the investigator must know the date and time of the IP addresses association with the illegal activity. The summons or subpoena will then include that date/time information which allows the dynamic provider to search its records to see what customer was logged in and using that IP number at that date and time.

Regardless of whether the IP address associated with the illegal activity is static or dynamic, it is incumbent upon the investigator to connect the IP address associated with the illegal activity with a specific user and location during the period of time the illegal activity took place if a search warrant is planned. This is true to ensure that it is the correct individual and physical address that is searched.

In other words, there needs to be a link via IP numbers from the illegal activity to the suspect's residence, business or other physical location. That link may be a series of IP addresses that trace back to a residence (as opposed to one direct link from the residence to the activity) but there must, in the final analysis, be a link between the activity in question and the location to be searched or there is a substantial risk of entering the wrong residence.

Pages 21 and 24 of the affidavit list two separate IP addresses, 67.174.220.41, for a PayPal transaction on 1/26/07 and 67.188.84.72, for a PayPal transaction on 1/29/07, both alleged to be associated with the purchase of child pornography. These IP addresses are currently leased by Comcast and currently show to separate geo locations, or point of origin, one in Oakland California and one in San Jose California. These geo locations may indeed be different today than they were in January of 2007 but nevertheless, reading the affidavit, there is no mention of any subpoena being sent or received to determine if it was the defendant's Comcast account that was using those IP numbers on those specific dates. Thus, there is no actual connection made between the IP addresses associated with these PayPal transactions and Mr. [redacted] or Mr. [redacted]'s residence.

These IP numbers are critical pieces of information that link the illegal transaction with a specific user and location. I noted that the affidavit made reference to what IP addresses are, and that there were IP addresses associated with these transactions but never linked the two together. These statements, I believe would contribute to confusion in attempting to understand the affidavit's probable cause because in reading these sentences one could easily assume that these numbers had been connected with Mr. [redacted]'s residence or business when in fact they had not.

It is a well-known and highly circulated fact that people's identities and credit card information, particularly through entities such as PayPal, are stolen and used on the Internet for illegal activity thousands of times a day. Certainly when the activity involves using a credit card for access to an illegal child pornography web site, using someone else's identifying information and Internet payment method (be it credit card or PayPal account) over your own would be highly preferred.

Typically, if a person's credit card or other type of online payment method information is stolen for fraudulent or illegal use, the thief will need to use the name, physical address and email

address associated with the account for on-line transactions because the account or card number will not work if they do not. Simply having the account information (such as with PayPal) or credit card number is usually not sufficient and the thief will also need to use the card holders name and addresses as well. This is why when credit card numbers are bought and sold on line, they are relatively worthless unless the purchaser also receives the name, billing address and CVN (card verification number) along with the card number and/or other account information itself.

It is primarily for this reason that relying on information provided by the user of a credit card, or on-line payment agency such as PayPal that is associated with criminal activity is unreliable. Taking for granted that the registration information provided by the user of a credit card number or financial accounting agency that uses credit card information such as PayPal accessing an illegal web site is absolutely true, without associating evidence linking that access to the suspect via IP addressing, is, in my opinion likely to lead to an executed warrant on what is essentially a *victims* residence or business.

CONCLUSION

My review of the search warrant affidavit in this case revealed that there was no stated IP address connection that linked either the offending web page or associated PayPal accounts with either Mr. [redacted]'s home or business locations. What it appeared was relied upon was textual information which although accurate in and of itself, did not mean it was the defendant who did so. Relying only on the fact that a person's on-line payment method (be it a credit card or PayPal) was used for an illegal transaction is, in my opinion, inherently unreliable and should not be used as the bases for a search warrant.

I also believe that the affidavit was confusing to read because making multiple references to IP addresses, could lead a reader to believe that the investigator had made the critical link between the criminal activity on the offending web pages and Mr. [redacted] when in fact they had not.

This issue is extremely important. Without requiring investigators to provide specific evidence linking the defendant (and his physical location) to the illegal acts, every citizen with an on-line identity runs a substantial risk of having their houses raided, personal property seized, and arrests made as the result of someone else using their personal identification to commit crimes.

It is extremely important for the safety and well being of every American whose identity is publically available (and most all are) that law enforcement entities be required to take steps to insure that it is the subjects residence where the illegal acts are occurring from. This is easily done and so critical to both homeowner and officer safety that it should not be an issue in probable cause affidavits. To rely solely on personal identifiers used by the person committing the illegal acts is inherently unreliable and can easily lead to misguided search warrants and the arrest of persons who are in actuality, victims.

_____ Date:_____

Marcus Lawson